

ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction, algorithm logic, and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow. The cryptographic instruction prescribes one of the cryptographic operations and one of a plurality of cryptographic algorithms. The algorithm logic is operatively coupled to the cryptographic instruction and directs the computing device to execute the one of the cryptographic operations according to the one of a plurality of cryptographic algorithms. The execution logic is operatively coupled to the algorithm logic and executes the one of the cryptographic operations.